Council of Europe convention 108+

de Terwangne, Cécile

Published in:
Computer Law and Security Review

DOI:
10.1016/j.clsr.2020.105497

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Council of Europe convention 108+: A modernised international treaty for the protection of personal data

Cécile de Terwangne

Faculté de Droit Université de Namur, 61 rue de Bruxelles, B-5000 Namur, Belgium

ARTICLE INFO

Keywords:
Data protection
Council of Europe Convention 108
Modernised Convention 108
Personal data
Informational autonomy
Data subject's rights
Data security
Transborder data flows
Supervisory authority
Convention Committee

ABSTRACT

The Council of Europe has modernized its Convention 108 for the protection of individuals with regard to automatic processing of personal data: in 2018 it adopted Convention 108+. The modernised version of Convention 108 seeks to respond to the challenges posed, in terms of human rights, by the use of new information and communication technologies.

This article presents a detailed analysis of this new international text. Convention 108+ contains important innovations: it proclaims the importance of protecting the right to informational autonomy and human dignity in the face of technological developments. It consolidates the proportionality requirement for data processing and strengthens the arsenal of rights of the data subjects. It reinforces the responsibility of those in charge of data processing as well as its transparency. It requires notification of security breaches. It strengthens the independence, powers and means of action of the supervisory authorities. It also strengthens the mechanism to ensure its effective implementation by entrusting the Committee set up by the Convention with the task of verifying compliance with the commitments made by Parties.

1. Introduction

Born on 28 January 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter "Convention 108") served as the foundation for the data protection regimes of the 47 member States of the Council of Europe, as well as several countries far beyond the European borders.

This Convention is the only legally binding international treaty on the protection of personal data. It has been modernised in order to meet the new challenges arising from the tremendous developments that have taken place since its adoption. The legal responses taken to protect individuals in 1981, at a time when there was no Internet, social networks, big data, connected objects or geolocation, proved insufficient in the current interconnected world where personal data has become the object of all covetousness. The changes that have emerged during these decades relate to the volume of data processed, the variety of actors, the scale of operations on data, the economic value attached to data, the threats to data, the overall availability of data in time and space, etc.[1]

The time for revision had also come for other international or regional legal instruments in this area. For example, the Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, dated 23 September 1980, were revised on 11 July 2013. As to the European Union's Directive

E-mail address: cecile.deterwangne@unamur.be

[1] See OECD, The OECD Privacy Framework, 2013, 3-4.

https://doi.org/10.1016/j.clsr.2020.105497

95/46[2], it was replaced on 25 May 2018 by the highly publicised General Data Protection Regulation (GDPR).[3]

The work to modernise Convention 108[4] was carried out by the Consultative Committee set up under the Convention, and continued by an intergovernmental committee (Ad Hoc Committee on Data Protection - CAHDATA)[5]. It led to the adoption by the Committee of Ministers of the Council of Europe, on 18 May 2018, in Elsinore, Denmark, of the Protocol of Amendment to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[6] This Protocol was open for signature on 10 October 2018.

The result of this modernisation work is the subject of the analysis developed in the following pages. The focus will be on the text of the amending protocol of 10 October 2018, which the Council of Europe services have named "Convention 108+", in view of effective communication, supported by the information provided in the explanatory report on this modernised Convention 108. It should be noted that, in an unusual development, the Committee of Ministers has endorsed the explanatory report. Therefore, "the explanatory report forms part of the context in which the meaning of certain terms used in the Convention is to be ascertained (Article 31, paragraphs 1 and 2 of the United Nations Vienna Convention on the Law of Treaties)".[7]

2. Universal standard

As expressly stated in the Preamble to Convention 108+, the States signatories to the Convention recognise "that it is necessary to promote *at the global level* the fundamental values of respect for privacy and protection of personal data, *thereby contributing to the free flow of information between people*".[8]

Although the principles of personal data protection stem from the European melting pot, they are undeniably destined to have an effect well beyond European borders. Convention 108 is, to date, the only legally binding text with a universal vocation in the field of data protection[9]. This text, in its original version of 1981, has been ratified by the 47 member States of the Council of Europe and is open for signature by non-member States.

Article 23 of the Convention governs the accession of non-member States of the Council of Europe in the following terms: "1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee."

To date, this procedure has resulted in the ratification of the Convention by Uruguay, Mauritius, Senegal, Tunisia, Cape Verde, Mexico, Argentina and Morocco.[10]

3. Convergence of the European texts: Convention 108(+) and GDPR

The two European regional institutions, the Council of Europe and the European Union (EU), have both had legislative action on data protection for several decades. While the Convention adopted by the Council of Europe sets out general principles, the EU texts (Directive 95/46 and GDPR) elaborate a detailed legal regime for data protection. That said, the texts adopted on both sides have unavoidable links and demonstrate the reciprocal influence of the two institutions. The national legislations adopted by the European States in the late seventies and eighties presented too many disparities, which was detrimental to the development of the European common market[11]. The EU then adopted Directive 95/46 with a view to harmonizing the data protection regimes of the EU member States[12]. This Directive clearly stated that it intended to give substance and amplify the principles contained in Convention 108[13].

Directive 95/46 provided additions to the data protection principles of Convention 108 in view of the developments in technology and practices that had taken place since 1981. These additions concerned in particular the necessity to set up independent supervisory authorities to ensure compliance with data protection principles and the need to adopt a restrictive regime to regulate transborder data flows to third countries. Following this model, the Council of Europe improved its original convention by adopting on 8 November 2001 the

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 , 23 November 1995.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4 May 2016.

[4] See Council of Europe, Data Protection, Modernisation of Convention 108: Background, https://www.coe.int/en/web/data-protection/background-modernisation.

[5] Terms of reference 2013 of the Ad hoc Committee on Data Protection, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066d6af; Information document on the Ad hoc Committee on Data Protection, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066d0b6.

[6] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), 10 October 2018, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223

[7] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Explanatory report, paragraph 6.

[8] Emphasis added in italic.

[9] Jörg Polakiewicz, "Convention 108 as a global privacy standard?", International Data Protection Conference, 17 June 2011, available at https://rm.coe.int/16806b294e.

[10] By order of accession to Convention 108.

[11] See recitals 7 and 8 directive 95/46/EC.

[12] Recital 8 directive 95/46/EC.

[13] Recital 11: "Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data".

Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS n°181)[14].

Fifteen years later, both institutions recognized the necessity to deeply modernise their respective legal instrument. At the EU level, this lead to the adoption on 27 April 2016 of the General Data Protection Regulation. The change from a directive to a regulation was aimed at achieving an ever greater uniformization of the EU legal landscape in the field of data protection. The revision action undertaken at the level of the Council of Europe ensured synchronization with the EU reform that enabled to maintain the consistency between both frameworks[15]. As a result, the coherence and compatibility between both European legal frameworks have been preserved. With regard to the nature of the legal instruments adopted in the two different European contexts, it should be noted that Convention 108+ is not a self-executing treaty and needs implementing legislation while GDPR is directly applicable even if some complementing legislation at national level is possible for certain provisions.

4. Values linked to the protection of personal data: human dignity and personal autonomy

4.1. *Human dignity*

The preamble of Convention 108 in its modernised version solemnly affirms "that it is *necessary to secure the human dignity* and protection of human rights and fundamental freedoms of every individuals …".[16]

From the outset of the new text, the need to guarantee human dignity with regard to the processing of personal data is being recognised. It is a reminder that the human being must remain a subject and not be reduced to a mere object, be it an object of algorithmic deduction, control or surveillance. The Explanatory Report of the modernised Convention 108 puts it this way: "[h]uman dignity requires safeguards to be put in place when processing personal data, in order for individuals not to be treated as mere objects".[17]

This proclamation of the fundamental value of human dignity at the outset of Convention 108+ is undoubtedly particularly necessary today in the face of automated decisions, the use of artificial intelligence fed by massive data (Big Data), the implementation of large-scale information systems, etc. It is in particular through the requirement that the fate of an individual should not be decided exclusively by software (the right not to be subject to a fully automated decision)[18] that the protection of human dignity will be ensured.

4.2. *Personal autonomy*

After affirming the need to guarantee human dignity, the preamble to Convention 108+ goes on to stress the need to guarantee also "the protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, *personal autonomy, based a person's right to control of his or her own personal data and the processing of such data*".[19]

Convention 108+ is about data protection notably as a right of control guaranteed to individuals based on their personal autonomy or personal self-determination. Data protection is indeed an offshoot of the right to privacy taken in this dimension of personal autonomy rather than in the sense of a confidentiality requirement (sense traditionally attached to the notion of privacy). The right to data protection is linked to a right to 'informational self-determination' that has been recognized as part of the right to privacy [20] by the European court of Human Rights.[21]

5. Scope of Convention 108+ and main concepts

5.1. *Scope of application*

5.1.1. *A particularly broad scope of application*

The Convention is applicable to all data processing activities, carried out in both the public and private sectors. It is therefore all processing of personal data which is covered by the rules of protection contained in the Convention. All fields of activity in which data processing is carried out are covered.

The Convention differs in this respect from other legal instruments such as the GDPR adopted by the European Union. Unlike the latter, the scope of the Convention covers data processing in the fields of justice, combating crime, defence, public safety and State security.[22] Exceptions to the provisions which might hamper the effectiveness of action in these fields, or which would undermine the separation of powers, are certainly provided for in the text,[23] but there is no longer

[14] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181.

[15] Even if both texts are consistent, some differences are noticeable, see Greenleaf, Graham, Convention 108+ and the Data Protection Framework of the EU - Conference Presentation 'Convention 108+ Tomorrow's Common Ground for Protection' (Council of Europe, Strasbourg, 21 June 2018), UNSW Law Research Paper No. 18-39, Available at SSRN: https://ssrn.com/abstract=3202606, p. 5.

[16] Emphasis added in italic.

[17] Explanatory report, paragraph 10.

[18] See *infra*.

[19] Emphasis added in italic.

[20] ECtHR [GC] *Satakunnan Markkinapörssi oy and Satamedia oy v. Finland*, 27 June 2017, Appl. n° 931/13, § 137: "[…] Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged." See also ECtHR [GC], *Evans v. UK*, 10 April 2007, Appl. n° 6339/05 ; *Tysiac v. Pologne*, 20 March 2007, Appl. n° 5410/03 ; *Daroczy v. Hongrie*, 1 July 2008, Appl. n° 44378/05.

[21] On numerous occasions, the European Court of Human Rights referred to Convention 108 in its judgments as a "relevant international instrument" to define the protection afforded under article 8 ECHR. "In the particular context of data protection, the Court has, on a number of occasions, referred to the Data Protection Convention" (ECtHR [GC] *Satakunnan Markkinapörssi oy and Satamedia oy v. Finland*, 27 June 2017, Appl. n° 931/13, § 133).

[22] See Article 3.1 of Convention 108+.

[23] See article 11 and article 14.4.c, of Convention 108+.

any question, as in the past,[24] of allowing a Party to fully exempt from the scope of the Convention categories of processing, such as those carried out by services responsible for State security.

Moreover, not only fully or partially automated processing of personal data falls within the scope of the Convention, but from now on also the processing of personal data not involving any automated process but relying on personal data contained in "a structured set of such data which are accessible or retrievable according to specific criteria".[25] By way of example, registers and directories, alphabetical lists, structured files or trombinoscopes, even if entirely on paper, fall within the scope of the Convention.

5.1.2. *Jurisdiction criterion*

It was decided in the course of the work on revising the Convention to refer to the concept of 'jurisdiction' rather than 'territory' when defining the scope of application of Convention 108+. Thus, while according to the 1981 text, "[t]he purpose of this Convention is to secure *in the territory of each Party* for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")",[26] Article 3 of Convention 108+ states: "Each Party undertakes to apply this Convention to data processing subject to *its jurisdiction* in the public and private sectors, thereby securing every individual's right to protection of his or her personal data."

Preferring the criterion of jurisdiction to that of territory should offer a better capacity to adapt the text to a changing reality that increasingly disregards a territorial anchorage.

An important clarification should be noted: the modernised Convention 108 expressly states that "[t]he purpose of this Convention is to protect every individual, *whatever his or her nationality or residence*, with regard to the processing of their personal data".[27] Protection is therefore offered as soon as data processing falls within the jurisdiction of a State or an international organisation Party to the Convention, regardless of the nationality or residence of the natural persons whose data are processed.

5.1.3. *The only total exclusion from the scope of application: data processing carried out in the course of purely personal or household activities*

Convention 108+ does not apply to data processing carried out by a natural person in the course of purely personal or household activities.

This exclusion from the scope of application should be clearly defined, given the scope that personal activities can nowadays take on when they are carried out, no longer in the privacy of a notebook, diary or photo album on paper, stored in a drawer, but by making use of the very effective online services which make it possible, in particular, to disseminate data on others via social networks or to store photos in the cloud.

According to the Explanatory Report of the modernised Convention, the data processing covered by the exemption relates to activities in the personal sphere and connected with the exercise of private life. In this sense, "personal or household activities" should be understood as "activities which are closely and objectively linked to the private life of an individual and which do not significantly impinge on the personal sphere of others. These activities have no professional or commercial aspects and relate exclusively to personal or household activities, such as storing family or private pictures on a computer, creating a list of the contact details of friends and family members, correspondence, etc."[28] For data sharing to be considered as taking place within the private sphere - and therefore outside the scope of the Convention - it must take place, for example, "between a family, a restricted circle of friends or a circle which is limited in its size and based on a personal relationship or a particular relation of trust".[29]

Thus, the exemption will not be applicable for personal data "made available to a large number of persons or to persons obviously external to the private sphere, such as a public website on internet".[30]

5.2. *Definition of the main notions*

5.2.1. *Notion of personal data*

The notion of "personal data" includes any information relating to an identified or identifiable individual (referred to as the "data subject").[31] It is a particularly broad concept since, far from being limited to private or confidential information, it applies to any information as long as it can be directly or indirectly linked to a living individual.[32]

The notion covers all types of information: confidential, private, professional, commercial or public. On this last point, it should be made clear that there is no question of depriving of all protection the data disseminated or made freely accessible on websites or on public pages of social networks.

The notion of personal data also covers any form of information (written, photographic, sound, location data, online behavioural data, biometric data, etc.).

Finally, it covers both data that result from objective, verifiable and questionable elements, and subjective data containing an evaluation or judgement about someone.

The important element to define the notion of personal data is that the person to whom the information relates should be identified or identifiable. The identification in question should not be understood as the establishment of the civil identity of an individual, but as the individualisation of that person, the ability to distinguish and treat him or her differently from others. "This "individualisation" could be done, for

[24] See Article 3.2. a, of Convention 108 of 28 January 1981.
[25] Article 3.1 of Convention 108+. Explanatory report, paragraph 21.
[26] Article 1 of Convention 108.
[27] Article 1 of Convention 108+.
[28] Explanatory report, paragraph 27.
[29] *Ibidem*.
[30] Explanatory report, paragraph 28.
[31] Article 2.a of Convention 108+.
[32] Explanatory Report, paragraph 30. We will be careful not to reduce the concept of personal data to identifying data only. Any information relating to an individual is to be considered as personal data as soon as this individual is identifiable (by the possible intervention of other data). Thus the words spoken by a participant in a meeting and recorded in the minutes are personal data as much as the name of this participant appearing in the minutes.

instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, a pseudonym, biometric or genetic data, location data, an IP address, or other identifier)".[33]

If the identification of the data subject requires unreasonable time, effort or resources, the data subject will no longer be considered "identifiable" and the data relating to him or her will be deemed anonymous. "The issue of what constitutes "unreasonable time, efforts or resources" should be assessed on a case-by-case basis. For example, consideration could be given to the purpose of the processing and taking into account objective criteria such as the cost, the benefits of such an identification, the type of controller, the technology used, etc."[34] Moreover, technological advances may cause fluctuations in what should be considered as "unreasonable time, effort or resources".

5.2.2. *Notion of data processing*

The notion of "data processing" has taken the place in the modernised version of the Convention of that of "automated file" used in the initial text but which no longer corresponded to current technological realities.

According to Article 2, b. of Convention 108+, "data processing" means "any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data".

The operations falling within the notion of data processing are therefore particularly varied and range from the collection to the destruction of data. In fact, anything that can be done with personal data, any kind of actions or uses of data falls within the definition of "data processing".

5.2.3. *Notions of controller and processor*

The two main categories of actors involved in the processing of personal data are the controller, and possibly, the processor.

The controller: According to Article 2, c. of the Convention, the concept of controller means "the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing".

Thus, while this main actor was identified in the initial version of Convention 108 as the person competent to decide on the purpose of the automated file, the categories of data concerned and the operations applied to them, this time a less detailed criterion is used, but intended to shed more light on the decisive role of the data controller with regard to the processing operation carried out on the data. It is therefore the person who exercises the power of decision on this processing operation. This power of decision may relate to the reasons justifying the processing, i.e. its purposes, as well as to the means used to process the data. Account may also be taken of whether or not to control the processing methods, the choice of data to be processed and who is allowed to access it.[35]

The identification of the controller may result from a formal designation or from factual circumstances to be assessed on a case-by-case basis.[36]

It should also be noted that the role of controller may be held by several persons jointly, the "co-controllers"[37] who are either jointly responsible for the same processing operation or in charge of different aspects of a processing operation.[38]

The processor: The inclusion of the notion of processor in the list of definitions in Convention 108+ responds to the need to identify actors who now play a decisive role in data processing. According to Article 2, f. of the Convention, this refers to "a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller".

It therefore refers to the person, in the broadest sense, who works on behalf of the controller, to carry out the (usually technical) tasks which the controller is not able to perform and which he or she delegates to him or her. The processor is a person external to the controller and cannot be an employee of the controller. He must carry out the processing operations in accordance with the instructions of the controller. These instructions shall lay down the limits to the authorised use of personal data by the processor.[39]

This category of actors plays a prominent role in today's context, in particular in the provision of hosting, cloud, social networking, etc. services. It has therefore proved essential to include processors in the text of the Convention in order to provide a framework for their involvement in data processing and to give them certain responsibilities (see below on the obligations provided for in Article 10 of the Convention). This is the case even if practice has revealed the difficulties of application that the notion raised. Indeed, it is not always obvious to distinguish between the notions of controller and processor. This is particularly true when dealing with a complex organisation such as a multinational company or a group of companies or when the same actor assumes several roles (such as Facebook).

6. Basic principles of protection

A set of basic principles must be respected in order to achieve the protection of personal data undergoing processing. This catalogue of principles and requirements is set out in Chapter 2 of Convention 108+. It concerns first of all the conditions for the legitimacy of data processing (set out in point 6.1. below) and data quality requirements (point 6.2.) as well as the enhanced protection regime for sensitive data (point 6.3.). It continues with the obligations of security and transparency. A series of rights also guarantee data subjects' information and thus their power of decision, action and supervision as to the fate of their data. These obligations and rights are set out in Chapters 7 and 8 below.

These principles, obligations and rights are not absolute. Exceptions to some of the conditions for the legitimacy of data

[33] Explanatory Report, paragraph 18.
[34] Explanatory Report, paragraph 17.
[35] Explanatory Report, paragraph 22.
[36] *Ibidem.*
[37] *Ibidem.*
[38] *Ibidem.*
[39] Explanatory Report, paragraph 24.

processing (the requirement of fairness, the purpose principle and the data quality requirement), as well as to the obligation of transparency and to the rights of data subjects, are provided for. They are described in Chapter 9 below.[40][41]

6.1. *Conditions for the legitimacy of data processing operations*

6.1.1. *Respect for the principle of proportionality*

The modernised version of Convention 108 contains a particularly important provision which could play a crucial role in the development of data processing operations that undermines the balance between the quest for efficiency and the protection of rights and freedoms (in the public sector) or between economic interests and the protection of those same rights and freedoms (in the private sector). Since the 'technically possible' is constantly being taken further and the economic interests linked to the exploitation of personal data are ever greater, this provision makes it necessary to reflect on the acceptability of the envisaged information systems and uses of data.

This is the express formulation of the condition of proportionality of data processing. Thus, according to Article 5.1 of the Convention, "data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake".

Any data processing must therefore be proportionate, i.e. relevant to the legitimate purpose pursued and limited to what is necessary with regard to the interests, rights and freedoms of the data subjects or the public interest. It must not lead to a disproportionate interference with those interests, rights and freedoms.[42]

Article 5(1) stipulates that the principle of proportionality must be respected at all stages of processing, starting with the initial stage, i.e. when a decision is taken on whether or not to process the data,[43] and then at each operation carried out on the data, in particular when the data are used, disclosed to a third party or linked to other data.

It is therefore now particularly clear that all the rights and freedoms at stake must be weighed before any data processing is launched, and that operations on data can only be carried out if the result of the weighing is balanced. This is the case even if the consent of the data subjects has been obtained. Indeed, as the Explanatory Report points out, "[a]n expression of consent does not waive the need to respect the basic principles for the protection of personal data set out in Chapter II of the Convention and the proportionality of the processing, for instance, still has to be considered."[44] Thus, the requirement of proportionality may serve as a bulwark not only against the risks of certain developments (such as the unsuspected data processing that abounds on the Internet) but also against the very (abusive?) widespread use of data subjects' consent to process their data. While the presence of consent makes it possible to presume the legitimacy of a processing operation, balancing the interests involved and verifying the balance achieved offers a welcome safeguard when one considers the shortcomings too often attached to consent (insufficient information of the data subject, manifestation of consent inferred from the non-change of default conditions, etc.). Moreover, the consent expressed by the data subject reflects only the consideration of his or her own interests, rights and freedoms and not those of others or of the community. What one is willing to accept out of convenience or economic interest may not be desirable at the level of society as a whole. Such data processing could therefore be challenged on the grounds of non-compliance with the proportionality requirement.

6.1.2. *Need for a legitimate basis for data processing*

In its 1981 version, the Convention was silent on the need for a legitimate basis for data processing to be admissible. The version of 10 October 2018 corrects this situation and introduces a provision setting out the assumptions of legitimacy of personal data processing. Thus, whereas the Convention did not previously reserve any place for the consent of the individual, it now stipulates that data processing may only be carried out "on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law".[45]

Since it would not be appropriate for an international treaty to present too detailed a list of hypotheses retained, it is in the Explanatory Report that the clarifications as to the "other legitimate basis laid down by law" are to be found. The Explanatory Report states that "other legitimate basis laid down by law" include "*inter alia*, data processing necessary for the fulfilment of a contract (or pre-contractual measures at the request of the data subject) to which the data subject is party; data processing necessary for the protection of the vital interests of the data subject or of another person; data processing necessary for compliance with a legal obligation to which the controller is subject; and data processing carried out on the basis of grounds of public interest or for overriding legitimate interests of the controller or of a third party".[46]

As for consent, to be valid it must be specific, free, informed and unambiguous. For consent to be considered free, no undue influence or pressure (of an economic or other nature) may be exerted on the data subject, who must have a genuine choice and must be able to refuse or withdraw consent without suffering prejudice.[47] The data subject must also have received the necessary information on the scope and implications of his or her consent.[48] This requirement goes hand in hand with an information obligation on the controller (see below). Unambiguous consent must be given by means of a declaration (written, electronic or oral) or an affirmative action which clearly indicates acceptance of the processing of the data in question. Accordingly, "mere silence, inactivity or pre-validated forms or boxes should not, therefore, constitute

[40] See *infra*.
[41] Article 11. 1 of Convention 108+.
[42] Explanatory Report, paragraph 40.
[43] *Ibidem*.
[44] Explanatory Report, paragraph 44.
[45] Article 5.2 of Convention 108+.
[46] Explanatory Report, paragraph 46.
[47] Explanatory Report, paragraphs 42 and 45.
[48] Explanatory Report, paragraph 42.

consent".[49] Moreover, consent covers all data processing operations that serve the same purpose, so that "in case of multiple purposes, consent should be given for each different purpose".[50]

6.1.3. *Fairness and transparency of data processing*

The requirement of fairness[51] implies that data processing must be carried out transparently for the data subjects and without deception. Data processing may not be carried out without the knowledge of the data subjects. The principle of fairness is closely linked to the duty of transparency. This duty of transparency implies that certain information should be provided spontaneously by the controller to the data subjects.[52] The idea is to inform data subjects fairly of the fate awaiting their data.

Fair processing of data is not limited to the moment of collection but must be guaranteed at all stages of collection.

It is an issue of fairness that was at the heart of the "Cambridge Analytica" scandal[53]: Facebook users were invited to answer a personality test for which they were led to believe that they were operating within the framework of an academic study and that the purpose was therefore academic, whereas in reality the purpose of the data collection was commercial and political prospecting.[54] It was also a lack of fairness that was reproached to Facebook - again - because of its collection (thanks to the social module "datr") of data on Internet users not registered on this social network and browsing outside Facebook, and therefore not expecting Facebook to collect traces of their browsing.[55]

6.1.4. *Compliance with the purpose specification principle*

As a fundamental principle of data protection, the purpose specification principle requires that personal data must be "collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes".[56] Requiring data controllers to determine from the outset the precise purpose of their action provides a common thread that will make it possible to know what data can be collected and used to serve that purpose, what actions can be carried out with the data, to whom the data can be communicated and how long they can be kept. Only operations and communications compatible with the original purposes are permitted.

The fact that the purpose must be explicit supports the desire for transparency to counteract the opacity that currently prevails in data processing.

The reference to "specified purposes" indicates that it is not allowed to process data for purposes that are not defined, imprecise or vague.[57] A sufficient level of precision of the purpose of data processing must be achieved. The mere reference to the tasks of an administrative service, for example, does not meet this requirement of specified purposes. Finally, for the purpose of data processing to be legitimate, a fair balance must be struck between the rights and interests of the data subject and those of the controller or the company.[58] A purpose that would cause undue harm to the data subjects will not be accepted as legitimate. At the level of purpose, the proportionality requirement exists for all data processing (cf. point 1 *supra*).

The purpose specification principle also implies that only uses compatible with the purpose or purposes determined and announced at the outset, at the time of collection, are permitted.[59] The notion of "compatible" use must be understood taking into account the need for transparency and fairness of data processing.[60] In particular, personal data must not be further processed in a way that the data subject might consider unexpected, inappropriate or questionable.[61]

This aspect of the purpose principle is also reflected in the case law of the European Court of Human Rights. In the case of *M.S. v. Sweden*,[62] confidential, personal and sensitive medical data of a patient had been transferred from one public authority to another without her consent. According to the Court, "the subsequent communication served a different purpose" and "… the disclosure depended on a number of factors beyond her control".[63] Accordingly, the Court found that the dis-

---

[49] *Ibidem*.

[50] *Ibidem*.

[51] Article 5.4, a of Convention 108+.

[52] See Article 8 of Convention 108+.

[53] See C. Cadwalladr et E. Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", *The Guardian*, 17 mars 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; CNIL, « Affaire Cambridge Analytica/Facebook », 12 avril 2018, https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook.

[54] See É. DEGRAVE, « Cambridge Analytica: et la vie privée ? », *Journal de Droit Européen.*, 2018, 213.

[55] Deliberation of the CNIL's restricted composition SAN-2017-006 of 27 April 2017 deciding of a pecuniary sanction (150.000 €) against FACEBOOK INC. and FACEBOOK IRELAND https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000034728338&fastReqId=390211096&fastPos=2. Also see Civil Court of Brussels, 16 February 2018, n° 2016/153/A, https://www.privacycommission.be/sites/privacycommission/files/documents/jugement_facebook_16022018.pdf. E. Degrave, « Facebook, les cookies et la justice belge : le retour », Justice en ligne, 22 mars 2018, http://www.justice-en-ligne.be/article1044.html. Sanctions imposed are based on the French and Belgian data protection laws, which are complying with Convention 108+.

[56] Article 5.4, b of Convention 108+.

[57] Explanatory Report, paragraph 48.

[58] *Ibidem*. The case law of the European Court of Human Rights goes in the same direction: in its judgment *S. and Marper*, the Court thus affirmed that the processing of data must be proportionate, that is to say appropriate with regard to the legitimate aims pursued, necessary insofar as there are no other appropriate measures less detrimental to the interests, rights and freedoms of the persons concerned or of society, and that it cannot cause disproportionate harm to these interests, rights and freedoms in relation to the benefits expected by the controller (ECHR, Grand Chamber, 4 December 2008, *S. and Marper v. United Kingdom*, applications no. 30562/04 and 30566/04, paragraph 118).

[59] Article 5.1 of Convention 108+.

[60] Explanatory Report, paragraph 49.

[61] *Ibidem*. The Explanatory Report sets out a series of criteria to establish whether the use of the data for another purpose is compatible or not with the purpose of the initial collection. These criteria are: the link that may exist between the two purposes, the context, the nature of the data, the consequences of further processing and existing safeguards.

[62] European Court of Human Rights, *M.S. v. Sweden*, judgment of 27 August 1997, application no. 931/13.

[63] *Ibidem*, paragraphs 35 and 32.

closure of the data infringed the patient's right to privacy. For this infringement to be admissible, the disclosure of the data must be provided for by an accessible standard that is sufficiently precise.

Article 5.4. b, of Convention 108+ specifies that the further processing of personal data for archiving purposes in the public interest, for scientific or historical research or for statistical purposes is *a priori* considered compatible under two conditions:

- that additional safeguards apply. As examples of additional safeguards, the Explanatory Report cites "anonymisation of data or data pseudonymisation, except if retention of the identifiable form is necessary; rules of professional secrecy; provisions governing restricted access and communication of data for the above-mentioned purposes, notably in relation to statistics and public archives, and other technical and organisational data security measures"[64]; and
- that data processing operations " in principle, exclude any use of the information obtained for the purpose for decisions or measures concerning a particular individual".[65] Archiving, statistical and scientific research purposes cannot, in principle,[66] lead to individual decision-making or action.

Finally, it should be noted that from the purpose specification principle follows the requirement not to keep data longer than necessary to achieve the purpose(s).[67]

6.2. *Data quality requirements*

Already present in the 1981 version of the Convention, data quality requirements have stood the test of time and are still valid in the 2018 version. Personal data must therefore always be "adequate, relevant and not excessive in relation to the purposes for which they are processed"[68] and "accurate and, where necessary, kept up to date".[69]

In order to be considered adequate and relevant, the data must have a necessary and sufficient link to the purposes pursued.[70] In reality, it is often the case that information is collected that goes beyond what is relevant in view of the purpose pursued: an order form for a good asking for the date of birth, collecting an ID number for the granting of a loyalty card, surveillance camera of a house entrance overflowing into the neighbourhood, etc.

The requirement for non-excessive data, for its part, is an explicit invitation to moderation. This provision covers both quantitative and qualitative aspects of the personal data being processed.[71] This means, on the one hand, that care must be taken not to collect more data than necessary and, on the other hand, that even relevant data which cause excessive harm to the data subject must not be processed. This is the case in particular for the communication to the employer of an opinion of the occupational doctor which would reveal in detail the state of health of an employee. Although relevant to enable the employer to check the data subject's fitness for work, these medical data are excessive. Only the communication of a finding of aptitude or unfitness without any further development of the data subject's health is acceptable.

On the practical side, compliance with this minimisation requirement can be facilitated by the use of systematic anonymisation or pseudonymisation techniques or by a data-saving default setting.

6.3. *A more protective regime for sensitive data*

The identification of a special category of personal data to which a higher level of protection is reserved is linked to the increased risks of harm to individuals on the basis of the processing of such data. It is mainly the risk of illegitimate or arbitrary discrimination linked to such data that justifies the differentiated processing of such data. Such data furthermore present a risk of affecting the most intimate sphere of the data subjects as well as a serious risk of harm, in case of abuse, to the data subject.

The list of sensitive data is contained in Article 6. 1 of Convention 108+. A distinction is made between:

- data which are sensitive by nature and which are in all circumstances of a sensitive nature: genetic data and personal data relating to offences (including suspected criminal offences), criminal proceedings and convictions and related security measures;
- biometric data when processed for the purpose of uniquely identifying a natural person;
- sensitive data by virtue of the use to which it is processed: personal data for the information it reveals on racial or eth-

[64] Explanatory Report, paragraph 50.
[65] *Ibidem*.
[66] It may happen, for example in the context of medical research based on coded databases, that one decides, in the light of the research results, to go back to the patients to modify their treatment, and therefore take an individual measure.
[67] Article 5.4. e, of Convention 108+.
[68] Article 5.4. c, of Convention 108+.
[69] Article 5.4. d, of Convention 108+.
[70] Boulanger M.-H., De Terwangne C., Léonard T., Louveaux S., Moreau D., Poullet Y., « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 146.
[71] Explanatory Report, paragraph 52.

nic origin, political opinions, trade union membership, religious or other beliefs, health or sex life.[72,73]

Data in the latter category should only be considered sensitive in cases where it is precisely the sensitive piece of information contained in the data that is being processed. Thus, when the processing of recorded images is intended to reveal information on racial or ethnic origin, or on the health of the persons filmed, it is processing of sensitive data. Whereas it will be ordinary data processing if individuals are only filmed in a video-surveillance context for security purposes, without seeking to process the sensitive element contained in the images.[74]

A more protective regime than for ordinary data is reserved for sensitive data, given the higher risk that their processing entails for the data subject. Their processing is only allowed on condition that appropriate safeguards, in addition to those of the Convention, are provided for by law.[75] Two clarifications are made regarding the safeguards that must accompany the processing of such data. Firstly, as has just been said, the appropriate safeguards must be additional to the protective measures established by the Convention. It is therefore not sufficient to refer only to measures under the general regime to make the processing of sensitive data admissible. These may be legal or other safeguards. Secondly, the appropriate safeguards are presented as those that prevent the serious risk that the processing of sensitive data poses to the interests, rights and fundamental freedoms of the data subject, in particular the risk of discrimination.

[72] Genetic and biometric data are new in the list of sensitive data compared to the list of 1981. Data relating to convictions have been extended to offences, proceedings and security measures. As for the other data, they were already included in the initial list except the data revealing ethnic origin or union membership. However, the Explanatory Report to the Convention stated that this list should not be considered exhaustive and that States Parties could add other categories of data if the sociological context so required. The example given was precisely that of information on union membership. It was noted that in some countries this information was considered to entail risks to privacy, while in other countries it was only considered sensitive insofar as it was closely linked to political opinions. Some Parties had therefore already added them to the list of sensitive data.

[73] The European Court of Human Rights has also stressed the sensitive nature of several types of data, such as medical data (ECHR, 25 February 1997, *Z. v. Finland*), genetic and biometric data. It considered that "the conservation of fingerprints constitutes an infringement of the right to respect for private life" (ECHR, 4 December 2008, *S. and Marper, supra.*) which can therefore only be accepted subject to compliance with conditions of paragraph 2 of article 8 of the ECHR. According to the Court, "The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse. The above considerations are especially valid as regards the protection of special categories of more sensitive data and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family" (*Ibidem*, paragraph 103).

[74] Explanatory Report, paragraph 59.

[75] Article 6.2 of Convention 108+.

7. Security and transparency obligations - additional obligations

7.1. *Security obligation*

7.1.1. *Appropriate safety measures*

Personal data should be protected against unhealthy curiosity from inside or outside or against unauthorised manipulation, whether accidental or malicious. A duty to adopt security measures already existed in the original text of the Convention. It has been taken over in the modernised version of 2018 with, in passing, a clarification of the responsibility for security: it is the responsibility of the controller as well as of the processor, in cases where the services of a processor are used.

These actors must, in the words of Article 7.1 of Convention 108+, "take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data".

The security measures to be taken are of two kinds[76]: organisational measures (limiting the number of persons having access to data, using regularly renewed passwords, closing the premises where computers are located, etc.) and technical measures (frequently updated anti-virus program, firewalls, security backup, login, etc.). While the text merely states that the security measures should be "appropriate", the Explanatory Report specifies that the choice of security measures should take into account "the potential adverse consequences for the individual, the nature of the personal data, the volume of personal data processed, the degree of vulnerability of the technical architecture used for the processing, the need to restrict access to the data, requirements concerning long-term storage, etc.".[77] The security requirement can therefore be modulated according to the risks that the processing operation entails for the data subjects. Thus, the more sensitive the data involved and the greater the risks for the data subject, the greater the precautions to be taken. For example, data relating to a person's health used outside a medical context (e.g. by an insurance company to grant life insurance) will have to be subject to strict security measures.

It is noted that case law has already provided an interesting clarification of the scope of this requirement. It follows that security measures must not only prevent unauthorised access but also allow data subjects to control accesses to the data that have taken place. Only obtaining information on access to the data, by X and Y allows the data subject to verify the effectiveness of the security measures and allows him/her to exercise control or command over his/her own information. It was in this sense that the European Court of Human Rights ruled in the case of *I v. Finland*, condemning that State for allowing a public hospital to set up a data security system which only keeps in memory the traces of the last five accesses to the data and which, moreover, erases all traces of access once the data have been placed in the archives.[78]

[76] Explanatory Report, paragraph 62.

[77] *Ibidem*.

[78] European Court of Human Rights, *I. v. Finland*, judgment of 17 July 2008, application no. 20511/03, paragraph 41.

7.1.2. *Measures in the event of a security breach*

An additional paragraph has been added to Article 7 of Convention 108+ on data security. It concerns the obligation to report the occurrence of security breaches of a certain level of seriousness. The new rule reads as follows:

> "2. Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects."[79]

This requires notifying the supervisory authority of any data breach that is likely to seriously infringe the fundamental rights and freedoms of the data subject. As examples of a "serious" breach of the fundamental rights and freedoms of data subjects, the Explanatory Report cites the disclosure of data covered by professional confidentiality, or of data that could result in financial harm (such as credit card data) or cause damage to reputation, physical harm or humiliation.[80]

A data breach occurs when an unauthorized third party, such as a hacker, has accessed personal data by illegally breaking into a server. It also includes situations in which personal data have been lost (e.g. on CD-ROMs, USB sticks or other portable devices), or inadvertently or maliciously communicated by an authorised user in breach of the purpose specification principle or his/her duty of confidentiality (e.g. to reflect cases that have actually occurred: a bank data file transmitted to the tax authorities of a third country by a dismissed employee, as a form of revenge; the accidental publication on a website of the list of persons affiliated to a political party; the sending by a pharmaceutical company of an e-mail alert about a drug, revealing the names and contact details of all persons consuming that drug, etc.). If the consequences of these data breaches for the data subjects can be qualified as serious, the obligation to notify the problem will apply.

According to the Explanatory Report, reporting data breaches to the supervisory authorities is the minimum requirement. The controller should also be obliged to inform the supervisory authorities of the measures taken or envisaged to remedy the breach and to mitigate the potential consequences.[81] In addition, it may be necessary to inform the data subjects themselves, in particular when the data breach is likely to cause a substantial risk to their rights and freedoms, "such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage".[82] In such cases, data subjects should be informed of the measures to be taken to mitigate the adverse effects of the breach of their data.[83]

Finally, it should be noted that this obligation to notify data breaches is subject to the exception provided for in Article 11. 1 of the Convention, i.e. the exception on behalf of overriding public or private interests which would suffer from such transparency of data security breaches.[84]

7.2. *Obligation of transparency*

A data protection system that claims to be credible today can no longer, as in 1981, live with guarantees that are essentially based on the sole initiative of the data subject. It has become imperative, given the particularly opaque environment of current information systems, to make data controllers responsible for active transparency obligations. The data subject cannot take an interest in and obtain information about a processing operation of which he or she has no suspicion. How many data subjects will think that words entered in a search engine are recorded for months and linked to their identifier? Or that cameras are filming them when they are miniaturized and, given their power, placed at a good distance? Or that the gate they pass through reads the RFID chip in their passport? Examples of such situations where data subjects have no idea that their data is being processed until they have been informed of such processing are multiplied over and over again today.

It was therefore quickly decided when the Convention was being modernised to introduce an express obligation to inform the persons whose data are being processed, to be borne by the controller. The purpose of this information obligation is clearly "to act transparently in order to ensure fair processing and to enable data subjects to understand and thus fully exercise their rights in the context of such data processing."[85]

This obligation is set out in Article 8.1 in the following form:

"Each Party shall provide that the controller informs the data subjects of:

a His or her identity and habitual residence or establishment.
b The legal basis and the purposes of the intended processing.
c The categories of personal data processed.
d The recipients or categories of recipients of the personal data, if any; and
e The means of exercising the rights set out in Article 9.

as well as any necessary additional information in order to ensure fair and transparent processing of the personal data."

A range of information must therefore be spontaneously communicated to the persons on whom data are processed, subject to the possibility for the Parties to provide for exceptions in accordance with Article 11.1[86] and if the data subjects do not already have this information[87]: the name and address of the controller (or co-controllers), the legal basis and purposes of the processing, the categories of data processed and their recipients, and the means of exercising rights. This information, which must be easily accessible and comprehensible, may be provided in any appropriate format (via a website, technological tools on personal devices, etc.) provided that it

[79] Article 7.2 of Convention 108+.
[80] Explanatory Report, paragraph 64.
[81] Explanatory Report, paragraph 65.
[82] Explanatory Report, paragraph 66.
[83] Ibidem.
[84] On this, see *supra*, beginning of Chapter IV.
[85] Explanatory Report, paragraph 67.
[86] On this, see *supra*, beginning of Chapter IV.
[87] Article 8.2 of Convention 108+.

is presented effectively and fairly to the data subject.[88] among the "any necessary additional information in order to ensure fair and transparent processing of the personal data" is, inter alia, the length of time the data will be kept or information on the third countries to which the data will be communicated if they are actually intended to be sent abroad.

Two specific exceptions to this duty to provide information are provided for in addition to the possibilities for exceptions given by Article 11 of the Convention.[89] These specific exceptions are not covered by the justifications for exceptions allowed under Article 11.1, which are based on the protection of overriding public or private interests. These two exceptions apply only in the case of indirect collection of personal data, not in the case of the collection of personal data by a third party.

One of these exceptions takes into account material constraints: the controller is not obliged to provide the information when this is impossible or involves a disproportionate effort, because, the Explanatory Report states,[90] the data subject is not directly identifiable or has no means of contacting him or her. This impossibility may be practical (e.g. when a data controller only processes images and does not know the name and contact details of the data subjects) but may also be legal (e.g. in the context of a criminal investigation).[91]

The second exception is granted for processing operations provided for by law. The adage "no one is supposed to ignore the law" makes it possible to consider that citizens are already informed, but this is valid only on condition that the law in question is sufficiently precise and provides the necessary information to ensure that the persons concerned are fairly informed.

7.3. *Additional obligations*

A new provision, Article 10, has been introduced in the modernised Convention to add additional obligations to the transparency and security obligations.

The Parties are free to modulate these requirements according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controllers and processors.[92] This flexibility should avoid imposing material obligations that are too burdensome for certain types of data controllers, such as "small and medium-sized enterprises processing only non-sensitive personal data received from customers in the framework of commercial activities and not re-using it for other purposes".[93]

7.3.1. *Accountability principle*

First of all, it is a matter for data controllers and, where applicable, processors, to "take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11.3, in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention."[94]

This is a succinct formulation of what has been called the principle of accountability.[95] It requires that internal mechanisms be put in place to demonstrate the compliance of processing with the applicable provisions.

As examples of appropriate measures to ensure compliance by controllers and processors, the Explanatory Report mentions "training employees, setting-up appropriate notification procedures (for instance to indicate when data have to be deleted from the system), establishing specific contractual provisions where the processing is delegated in order to give effect to the Convention, as well as setting-up internal procedures to enable the verification and demonstration of compliance."[96]

It is also as a measure to facilitate the verification and demonstration of the conformity of data processing operations that it is proposed that the controller should appoint a data protection officer with the necessary means to fulfil his or her mandate.[97] The Explanatory Report states that "[s]such a data protection officer, whose designation should be notified to the supervisory authority, could be internal or external to the controller. "[98]

7.3.2. *Examination of the impact on fundamental rights and freedoms - obligation to minimise risks*

Before processing personal data, the controller has an obligation to examine the impact of the processing of personal data on the fundamental rights and freedoms of others and to design the processing so as to minimise that impact. Article 10.2 of Convention 108+ provides as follows: "controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and freedoms fundamental of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risks of interference with those rights and fundamental freedoms." In the course of this examination, the controller is called upon to assess compliance with the principle of proportionality at all envisaged stages of the data processing and to design the data processing in such a way as to avoid disproportionate interference with the rights of the data subjects.[99]

[88] Explanatory Report, paragraph 68.
[89] Article 8.3 of Convention 108+.
[90] Explanatory Report, paragraph 68.
[91] *Ibidem*.
[92] Article 10.4 of Convention 108+.
[93] Explanatory Report, paragraph 90.
[94] Article 10.1 of Convention 108+.
[95] The concept of "*accountability*" is not new and already appears in the OECD Guidelines of 23 September 1980 on the Protection of Privacy and Transborder Flows of Personal Data (article 14. on the accountability principle). On this concept see also Article 29 Working Party, Opinion No. 3/2010 on the principle of responsibility, WP 173 of 13 July 2010.
[96] Explanatory Report, paragraph 85.
[97] Explanatory Report, paragraph 87.
[98] *Ibidem*.
[99] Explanatory Report, paragraph 88.

This examination[100] of the impact on fundamental rights and freedoms can be done without excessive formalities and with the possible support of information systems developers, security specialists, lawyers or users.

7.3.3. *Privacy by design*

The principle of "Privacy by Design"[101] appears to be an indispensable requirement today to achieve effective privacy and data protection. This requirement to integrate privacy concerns within the systems, products and services created and from the very early stages of their design makes it possible to offer effective protection at a much lower cost than when privacy and data protection concerns have to be integrated later on, once the product has been designed and is operational.

Article 10. 3 of the Convention stipulates in this spirit that: "Each Party shall provide that controllers and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing."

Such measures may consist, for example, of "privacy-friendly standard configurations so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default), notably to avoid processing more data than necessary to achieve the legitimate purpose. For example, social networks should be configured by default configuration so as to share posts or pictures only with restricted and chosen circles and not with the whole Internet."[102] Or a technical configuration may facilitate the exercise of rights. For example, secure online access to data should be offered to data subjects whenever possible. There should also be easy-to-use tools allowing data subjects to take their data to another service provider or to keep the data themselves (data portability tools).[103]

8. The rights of the data subject

Everyone, regardless of age, residence or nationality, has rights vis-à-vis those who process data about them. Convention 108+ has remarkably expanded the list of guaranteed rights and strengthened the rights that already existed before.

The rights granted to the data subject are aimed in particular at ensuring transparency on request of data processing operations. This transparency must enable the data subject not only to be aware of, but also to control what is done with his or her data, to check compliance with the rules, to track down abuses or illegalities, to object, to correct errors. However, the first right enshrined in the list is linked to human dignity, i.e. the right not to be subject to an automated decision.

Before reviewing these rights, it should be recalled[104] that they are not absolute and that exceptions are permitted under the conditions set out in article 11 of Convention 108+. Thus, exceptions must be provided for by law, respect the essence of the fundamental rights and freedoms and be necessary in a democratic society for the protection of the overriding public or private interests listed in Article 11. 1, a and b.[105]

8.1. *The right not to be subject to an automated individual decision*

It seemed imperative for the authors of the modernisation of Convention 108 to enshrine, first and foremost, the right of every person to "not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration".[106]

Presented as the first right of the data subject, this right derives from the strong desire that man should not be entirely subjected to the machine. It is not desirable that a decision binding on an individual should depend solely on the conclusions of a machine. This is an expression of the pre-eminence to be accorded to human dignity.[107]

The technique is being increasingly used today to rely on a "computer" and the algorithms to decide what to do with an individual (whether or not to consider him as a tax evader, a marketing target or a potential terrorist traveller, etc.). In the name of human dignity, it is crucial for the individual to be able to effectively put forward his or her point of view and arguments and thus be able to challenge the decision. "In particular, the data subject should have the opportunity to substantiate the possible inaccuracy of the personal data before it is used, the irrelevance of the profile to be applied to his or her particular situation or other factors that will have an impact on the result of the automated decision."[108]

However, the prohibition to subject an individual to a fully automated decision shall not apply where the decision is authorised by a law to which the controller is subject.[109] In order for the automated decision to be admissible, that legal provision must provide for suitable measures to safeguard the rights and freedoms and legitimate interests of the data subject.[110]

---

[100] The authors of the modernisation of Convention 108 were attentive not to use the terminology used in the General Data Protection Regulation of the European Union (EU) 2016/679 which refers to the obligation to carry out an "analysis of 'data protection impact' (Article 35 GDPR). This, in order not to associate the impact assessment (resulting from Convention 108+) with a systematically cumbersome, expensive and restrictive formality, outsourced to be carried out by specialists. Risk assessment may be presented as such, in the case of complex and large-scale data processing, for example, but in many cases, it will be an informal internal process of healthy consideration of the consequences and risks associated with the intended data processing.

[101] On this principle, see A. Cavoukian, «Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices», December 2012, available at http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf ; B. Preneel et D. Ikonomou (dir.), Privacy Technologies and Policy : First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10–11, 2012, Revised Selected Papers, Berlin, Springer, 2014.

[102] Explanatory Report, paragraph 89.

[103] *Ibidem*.

[104] See Chapter IV, *supra*.

[105] See paragraph 91 of the Explanatory report.

[106] Article 9.1.a, of Convention 108+.

[107] See *supra* regarding *human dignity*.

[108] See paragraph 75 of the Explanatory report.

[109] Article 9.2 of Convention 108+.

[110] See paragraph 75 of the Explanatory report.

8.2. *Right of access*

For almost forty years, individuals have been guaranteed the right to be informed of the existence of data processing operations concerning them and of the content of the information being processed.

During the process of modernising the Convention, it was decided to enrich[111] this right of access and to include in it the right of obtaining on request all information which the controller is in principle obliged to communicate spontaneously to the data subjects.[112] Exceptions to this duty of spontaneous transparency existing, it is possible that an individual has not received any specific information about the processing carried out with his or her data and wishes to know, for example, the identity of the controller and his or her contact details, or the purposes of the processing, or the recipients of the data. He or she may therefore take the initiative to request this information.

Furthermore, the right of access has also been extended to cover access to the origin of the data. This information is indeed crucial as it is often the source of the data that intrigues and challenges the data subjects (how did they obtain this information? Who communicated it to them?). On the other hand, information on the source of the data makes it possible to verify the lawfulness of the communication or collection of the data and to possibly bring an action against the first holder of the data (which makes it possible to "stop the bleeding" if the latter unlawfully disseminates the data in question). Finally, in case of problems with the quality of the data and the need for corrections, it becomes possible to have these corrections made at the source, thus avoiding the further propagation of errors.

In the proposed new wording, the right of access therefore refers to the right of each data subject to "obtain, on request, at a reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her are, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8.1".[113]

8.3. *The right to know the reasoning underlying the processing of data*

Everyone has the right to obtain, on request, knowledge of the reasoning underlying the processing of data, where the results of the processing are applied to him or her,[114] including the consequences of such a reasoning and the conclusions that may have been drawn from it, notably when algorithms for automated decision-making are used, including in the context of profiling.[115]

This right is of great interest in view of the exponential deployment of the profiling phenomenon. This phenomenon is particularly widespread on the Internet, where it is used in the context of cyber-marketing or other areas of activity to analyse or predict aspects of the data subject's life. However, it is also a right to go beyond the limits of profiling, even if it is especially necessary in the face of the phenomenon where "profiles"[116] are used to make decisions about a person or to predict his or her personal preferences, behaviours and attitudes.[117] Clearly, even outside the profiling hypothesis, one may wish to understand what is happening by accessing the reasoning behind the data processing. Faced with the refusal of a credit, the results of an examination, the non-selection of an offer made in response to a call for tenders, etc., one may legitimately wish to know the criteria that played a role and the weight given to each of them in order to evaluate the ability to repay, correct and evaluate the examination or assess the quality of the offer.

This right to know the reasoning behind data processing is valuable in that it contributes to the informational self-determination of individuals as it allows them not only to know what is being done with their data but also to understand and possibly challenge it.

It should be noted that this right may be limited by the Parties to the Convention in accordance with the conditions laid down in Article 11 of the Convention for any restriction. This will notably be the case where it is necessary in a democratic society to guarantee "secrets protected by law", such as trade secrets.

8.4. *The right of objection*

It was decided to include the right of objection in the table of subjective rights intended to enable individuals to exercise control over the fate of their data. Every individual now has the right "to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her, unless the controller demonstrates legitimate grounds for the processing which override his or her interests, or rights and freedoms fundamental".[118]

This right is particularly justified when the processing of data is not based on the consent of the data subjects. Data subjects who have not been able to express their point of view at the start of the processing operation can use this right to put forward their arguments to the controller to convince him or her not to process their data. This right is particularly important in cases where the controller himself has carried out an *a priori* balancing of interests and has considered that the result was balanced and that he could legitimately process the data. Thanks to the right to object, the data subject has the op-

111 Article 9.1.b, of Convention 108+.
112 See *supra*.
113 Article 9.1.b, of Convention 108+.
114 Article 9.1.c, of Convention 108+.
115 See paragraph 77 of the Explanatory report.

116 'Profile' refers to a set of data characterising a category of individuals that is intended to be applied to an individual. (point 1.d. Appendix to Recommendation CM/Rec (2010)13, The protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010).
117 "Profiling" means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes. (point 1.e. Appendix to Recommandation CM/Rec (2010)13).
118 Article 9.1.d, of Convention 108+.

portunity to challenge the result of the balancing, at least in his or her case.

The data subject must give "grounds relating to his or her situation" which lead him or her to object to the processing of his or her data. It is for the controller who still wishes to continue processing the data in question to put forward overriding legitimate reasons and thereby prove that his or her legitimate interest takes precedence over the rights and interests of the data subject. According to the Explanatory Report, the exercise or defence of a right in a court of law as well as reasons of public security may be considered as overriding legitimate grounds for further processing of the contested data.[119]

It is clear that in the current context, where data processing without the knowledge of the data subjects is developing at an alarming rate, it is important to rebalance the situation of those involved by guaranteeing the right of data subjects to come forward and refuse the use of their data when they become aware of it. Individuals may also have been well informed of the planned processing operations but have not fully appreciated the fate of their data or the implications that these processing operations may have on other interests until a later date. In such cases too, the right of objection offers a timely solution.

In the case of processing of data for commercial purposes, an objection to such processing should unconditionally lead to the deletion of the personal data objected to, without the need for the data subject to give reasons relating to his or her situation.[120]

8.5. *The right of rectification and erasure*

The right of rectification and erasure has been granted to data subjects since the origin of Convention 108. Any person is therefore always recognised as having the right to "obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention."

The clarification that the rectification or deletion of data must be obtained "free of charge and without excessive delay" is a welcome addition to the modernised version of the Convention.

The right of rectification must therefore be exercised free of charge (if a data item is incorrect or if its processing is unlawful, it would be incomprehensible that one would have to pay to have an error rectified or to stop an unlawfulness). Correction or erasure must also be carried out without excessive delay, a concept which makes it possible to adapt the requirement of rapidity of reaction to situations. Thus, it will not be tolerated that the correction of a flagrant error relating to information disseminated on the Internet should take a week, whereas more time should be allowed for the contestation of data from an administrative service which requires verification.

Corrections and erasures obtained as a result of the exercise of this right "should, where possible, be brought to the attention of the recipients of the original information, unless this proves to be impossible or involves disproportionate efforts".[121]

Finally, it should be noted that it was decided during the work to modernise the Convention not to propose the explicit introduction of a "right to be forgotten" in the revised text of the Convention. It was in fact considered that the combination of the existing guarantees could offer effective protection to the persons concerned without infringing the right to freedom of expression. Thus, the right of rectification and erasure of incorrect, incomplete or unjustified data, combined with an effective right to object to the processing, provides a form of response to the concern about the right to be forgotten. Furthermore, the rule deriving from the purpose specification principle, imposing a shorter data retention period depending on the purpose of the processing operation to be carried out, leads to the erasure of data as soon as they are no longer useful for achieving the purpose of the processing operation.

8.6. *The right to a remedy*

According to Article 9.1. f, of the Convention, a remedy must be available to any person whose rights have been violated, such as where the controller has failed to reply or where the controller has failed to correct or delete data despite a request to that effect or has not stopped processing the data despite the data subject's objection.

This provision should be read in conjunction with Article 12 on "Sanctions and remedies". It provides that each Party undertakes to establish appropriate judicial and non-judicial remedies for violations of domestic law giving effect to the provisions of the Convention. The nature of the remedies established (civil, administrative, criminal) is left to the discretion of each State or international organisation Party.

It has been noted that "[m]ost countries which have data protection laws have set up supervisory authorities, generally a commissioner, a commission, an ombudsman or an inspector general. These data protection supervisory authorities provide for an appropriate remedy if they have effective powers and enjoy genuine independence in the fulfilment of their duties. They have become an essential component of the data protection supervisory system in a democratic society."[122] In order to be recognised as an appropriate remedy against violations of data protection rules, these supervisory authorities must be given the power to settle disputes, as well as powers of intervention and injunction.[123]

8.7. *The right to the assistance of a supervisory authority*

As mentioned above, individuals can turn to the national supervisory authorities to exercise their right of appeal against the non-respect of one of the rights guaranteed to them. Convention 108+ further provides that all persons shall be entitled "to benefit, whatever his or her nationality or residence, from

[119] See paragraph 78 of the Explanatory report.
[120] See paragraph 79 of the Explanatory report.
[121] Explanatory report, paragraph 81.
[122] Explanatory report of the 2001 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, point 5.
[123] See *infra* the analysis on supervisory authorities (chapter X).

the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention".[124]

This right to the assistance of the supervisory authorities is intended to ensure effective protection of the persons concerned. It will be particularly valuable in transfrontier situations, where the data subject resides in one country while the data controller is established in another country. In such circumstances, the data subject may submit his or her request through the authority of the State Party in which he or she resides.

This hypothesis, in which data subjects from another state may be effectively assisted, had already been envisaged in 1981 but was not formulated in law and did not yet involve the supervisory authorities, as the latter had no place in the Convention.

Article 14. 1 of the initial version of the Convention provided that "Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this Convention." The formula of Convention 108+ proposed in the form of a right and specifically targeting the assistance of the supervisory authorities is certainly more powerful.

This right may be limited under Article 11 or adjusted to safeguard the interests of ongoing judicial proceedings.[125]

9. Exceptions

As said earlier, exceptions to some of the conditions for the legitimacy of data processing (the requirement of fairness, the purpose principle and the data quality requirement), as well as to the obligation of transparency (including the reporting of security incidents of data breaches) and the rights of data subjects, are allowed subject to the conditions laid down in Article 11 of Convention 108+.

Thus, such exceptions are allowed only[126] if they are provided for by law, respect the essence of fundamental rights and freedoms and are necessary in a democratic society for the protection of overriding public (a) or private (b) interests:

(a) national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;
(b) the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

The Explanatory Report recalls that in order to be considered "necessary in a democratic society", a measure must pursue a legitimate aim and thus meet a pressing social need which cannot be met by less intrusive means. Furthermore, the measure must be proportionate to the legitimate aim pursued and the reasons put forward by the national authorities to justify it must be relevant and adequate. Finally, it must be established by an accessible and foreseeable law which must be sufficiently detailed.[127]

10. Transborder data flows

Prior to the modernisation of Convention 108, the issue of transborder data flows was the subject of two different provisions, one inserted in Article 12 of Convention 108 (for transborder data flows within Parties), the other in the 2001 Additional Protocol[128] (for flows to non-Parties to the Convention).

The two types of transfers of personal data are now dealt with together in a single provision: Article 14 of Convention 108+.

The regime for transborder flows aims at ensuring that personal data entering the jurisdiction of a Party to Convention 108+ continue to be protected with appropriate safeguards when, as a result of a transfer, they fall within the jurisdiction of a non-Party. The protection offered on the other side of the border "has to be of such quality as to ensure that human rights are not affected by globalisation and transborder data flows".[129]

10.1. *Notions of transfer of personal data and recipient*

It should be noted at the outset that if the notion of transborder flows appears in the heading of the provision, it is not mentioned afterwards. It is the notion of "transfer" that is present in the wording of the provisions on this subject. The Explanatory Report clarifies this notion as follows: "A transborder data transfer occurs when personal data is disclosed or made available to a recipient subject to the jurisdiction of another State or international organisation."[130] The notion of transfer therefore covers situations such as the making available of data in the cloud or on the Internet, where, without any actual movement of data, the data are made accessible to persons across borders.

The recipient of the data is referred to in the Convention as "the natural or legal person, public authority, service, agency, or any other body to whom data are disclosed or made available".[131] The Explanatory Report specifies that, depending on the case, the recipient may be a controller or a processor. For example, a multinational enterprise may send certain data of its employees to the Ministry of Finance of the State where the benefits took place, which will process them for tax purposes as a controller. It may also send them to a company offering storage services, which then acts as a processor.[132]

[124] Article 9.1.g, of Convention 108+.
[125] Explanatory report, paragraph 82.
[126] Article 11. 1 of Convention 108+.
[127] Explanatory Report, paragraph 91.
[128] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, CETS no. 181, 8 November 2001.
[129] Explanatory report, paragraph 103.
[130] Explanatory report, paragraph 102.
[131] Article 2.e of Convention 108+.
[132] Explanatory report, paragraph 23.

10.2. *Transfer of data between parties to Convention 108+*

Personal data shall enjoy freedom of flow between Parties to the Convention.[133] However, this freedom is not systematic, and the Convention envisages two possible ways of restricting data transfers. A State or organisation Party could, solely for the purposes of data protection, prohibit or make subject to special authorisation the communication or making available of data to a recipient under the jurisdiction of another Party to the Convention, in the event that:

- There is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, may lead to circumvention of the provisions of the Convention; to invoke this exception, the originating Party must have clear and reliable evidence that the transfer of data to the other Party could significantly undermine the protection afforded by the Convention to the data in question and that the likelihood of this happening is high. "This might be the case, for instance, when certain protections afforded under the Convention are no longer guaranteed by the other Party (for instance, because its supervisory authority is no longer able to effectively exercise its functions). "[134]
- The originating State must comply with harmonised rules of protection common to States belonging to a regional international organisation. It is therefore a question of being subject to the constraint of compliance with collective rules and not rules laid down individually and sovereignly by the State Party. An example of a common harmonised rule restricting flows between certain Parties is the regime provided for in Chapter V of the EU GDPR requiring an adequate level of protection to allow transborder data flows.[135]

Furthermore, a Party may restrict data transfers to another Party for a purpose other than data protection. For example, a State may prohibit transfers across borders in the name of national security, defence, public safety or other important public interests.[136]

10.3. *Transfers of data to a state or organisation that is not a party to Convention 108+*

For flows to a recipient under the jurisdiction of a State or organisation which is not a Party to the Convention, the rule is that they are allowed only if an appropriate level of protection based on the provisions of the Convention is guaranteed for the data transmitted.[137] It should be noted that, unlike the GDPR, which requires an "adequate" level of protection to allow flows of personal data outside the borders of the European Union, the Convention requires an "appropriate" level of protection. This difference is intended to avoid the same term having two different meanings depending on whether it would be used in the context of the European Union or the Council of Europe.

An appropriate level of protection may result from:

(a) The law of the State of the recipient or of the international organisation, including applicable international treaties or agreements, or
(b) Agreed *ad hoc* or standardised safeguards established by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing of the data (i.e. both by the person communicating or making accessible the personal data and by the recipient).

The supervisory authority must be informed of the *ad hoc* or standardised measures taken to ensure an appropriate level of data protection.[138] The authority does not have to give its authorisation but has the power to verify on the ground the quality and effectiveness of the measures taken and possibly to prohibit, suspend or condition a cross-border flow.

Finally, exceptions are provided for to allow the transmission of data without appropriate protection. This is the case if:

- The data subject has given his or her explicit, specific and free consent, after having been informed of the risks arising in the absence of appropriate safeguards; or
- Specific interests of the data subject so require in the particular case; or
- Prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; the Explanatory Report[139] specifies that, by this exception, personal data may be transferred on grounds similar to those listed in Article 11 of Convention 108+[140]; or
- Such a transfer constitutes a necessary and proportionate measure in a democratic society for freedom of expression.

11. The supervisory authorities

In 1981 no one thought of mentioning specific supervisory authorities in Convention 108. Twenty years later, the desire emerged to strengthen the effective protection of the individual through the creation of one or more supervisory authorities that contribute to the protection of the rights and freedoms of the individual with regard to data processing. The experience gained over the last 20 years had indeed shown

[133] Article 14.1 of Convention 108+.
[134] Explanatory report, paragraph 106.
[135] On the link between Convention 108+ and GDPR see: Ukrow, J., « Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108 », *EDPL*, 2018/2, p. 239-247.
[136] Explanatory report, paragraph 105.
[137] Article 14.2 of Convention 108+.
[138] Article 14.5 of Convention 108+.
[139] Explanatory report, paragraph 108.
[140] Grounds listed in Article 11.1 are : the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest, the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

that when they are equipped with effective powers and enjoy real independence in the exercise of their functions, such authorities have become an integral part of the data protection supervisory system in a democratic society.

An additional protocol was therefore drawn up and adopted on 23 May 2001 with a view to adding to the 1981 system of protection an obligation on the signatory states to set up a supervisory authority with the task of ensuring compliance with the protection regulations on their territory.

Nearly twenty years later, a new chapter on supervisory authorities transposes into Convention 108+, by fleshing them out, the provisions contained in this connection in Article 2 of the 2001 Additional Protocol.

Article 15 aims first and foremost to strengthen the independence of these supervisory authorities, in particular by specifying that these authorities must act independently and impartially in the performance of their duties and the exercise of their powers, without seeking or taking instructions from anyone.[141] The material guarantee of independence has also been envisaged and the text adds that the supervisory authorities must have the resources necessary for the effective performance of their functions and the exercise of their powers.[142]

Secondly, the text aims to strengthen the powers of the authorities. To this end, it recognises that these authorities must have powers of investigation and intervention, that they are competent in the field of transborder data flows in order to approve standardised legal clauses, that they must be able to take decisions on violations of the provisions of the Convention and in particular to sanction administrative offences, that they have the power to take legal action, and that they are responsible for raising awareness and educating people about data protection.[143]

It should be noted that the most remarkable strengthening is to be found in the autonomous decision-making and sanctioning powers of the supervisory authorities. Moreover, the authorities are entrusted with an educational mission in the field of data protection, which is certainly very relevant if one takes into account the current context in which data processing is carried out. The task of awareness-raising and education should be exercised towards the public, who should be made aware of the risks, whether hidden or not, arising from technical and societal developments. It would also be a question of raising awareness amongst controllers of the rules to be respected in order to ensure a balance between all the interests involved.

12. The Convention Committee

A Convention Committee with enhanced functions will take over from the Consultative Committee attached to the original Convention 108.

It will be composed of one delegate per Party and will be given an extended list of functions compared to the functions assumed by the Consultative Committee to date.[144] These functions include, *inter alia*: a power to make recommendations with a view to facilitating or improving the application of the Convention, a power to express opinions on any question relating to the interpretation or application of the Convention and on the level of protection of personal data provided by any candidate for accession (which may include recommendations on measures to be taken to achieve compliance with the provisions of the Convention) and a power to review regularly the implementation of the Convention by the Parties and to recommend measures to be taken in the event of non-compliance by a Party. The latter power of review is particularly important to ensure confidence between Parties, allowing the free flow of data between them.

13. Conclusion

At the end of this analysis of the modernised Convention 108, the main strengths of the new text to be highlighted are:

First of all, it is the only universally binding legal instrument on the protection of personal data. It offers a model regime of protection for all States and international organisations concerned with providing guarantees to individuals whose data are processed. This status of universal instrument therefore has the advantage that the inexorable increase in the number of Parties entails an enlargement of the geographical area in which transborder data flows are in principle free, except in case of a specific regional regime.

Moreover, the scope of the Convention covers all the activities of a Party, both those of the private sector and those of the public sector, and, among the latter, also personal data processing activities in the field of national security, defence and public safety, subject of course to such adjustments and restrictions to the principles of protection as are necessary not to hamper the effectiveness of the services' action.

A key element introduced by the revision of the Convention is that the protection of human dignity and personal autonomy when processing personal data is emphasised in the preamble to the text. These are the values at stake behind the rules set out in the Convention, in connection with the rights and fundamental freedoms of individuals, such as the right to privacy, freedom of expression and information, freedom of movement, the right to non-discrimination, the right to free elections, etc. The protection of these values of dignity and autonomy is essentially reflected in the rights guaranteed to data subjects and the obligations on controllers and their processors.

One provision is particularly important in Convention 108+.

This is Article 5.1, which proclaims the requirement of proportionality of any processing of personal data. Monitoring compliance with this requirement will enable the supervisory authorities and judges, where necessary, to act as a bulwark against any attempt to undermine human dignity or disregard the rights and freedoms of others.

[141] Article 15.5 of Convention 108+.
[142] Article 15.6 of Convention 108+.
[143] Article 15.2 of Convention 108+.
[144] Article 23, a to i, of Convention 108+.

Lastly, the strengthening of the role of the Convention Committee was particularly welcome. Its new power to examine the implementation of the Convention prior to any accession and in the form of monitoring once the Convention is ratified deserve special praise.

Declaration of Competing Interest

The author declares that she has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.